

## **CLAIM AMENDMENTS**

### **Claim Amendment Summary**

#### **Claims pending**

- Before this Amendment: Claims 1-35 and 37-48
- After this Amendment: Claims 1-5, 8, 10-11, 13-14, 17-21, 24, 26-27, 29-30, 22-25, and 37-43

**Non-Elected, Canceled, or Withdrawn claims:** 6-7, 9, 12, 15-16, 22-23, 25, 28, 21-32, and 44-48

**Amended claims:** 1-2, 8, 10-11, 13-14, 17-18, 24, 26-27, 29-30, 33, and 37

**New claims:** None

---

#### **Claims:**

##### **1. (Currently Amended)** A method comprising:

receiving a manifest defining a plurality of first and second code assemblies that are members of at least one application, wherein the manifest defines at least one trusted application and application evidence for making a trust decision;

evaluating the application evidence to determine if the at least one application is trusted;

generating a first and a second permission grant set for each the first and

the second code assembly, respectively, that is a member are members of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application; and

passing the permission grant to a run-time call stack;

calling the second code assembly by the first code assembly, the second code assembly attempting access of a protected file; and

calculating an intersection of the first and the second permission grant sets to determine whether the access to the protected file is permitted.

**2. (Currently Amended)** The method of claim 1 wherein the manifest further defines a plurality of code assemblies, the method further comprising evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

**3. (Original)** The method of claim 1 wherein evaluating application evidence is based at least in part on an XrML license.

**4. (Original)** The method of claim 1 further comprising evaluating application evidence at an application level and a code assembly level before

trusting the at least one application.

**5. (Original)** The method of claim 1 further comprising evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

**6. (Cancelled)**

**7. (Cancelled)**

**8. (Currently Amended)** The method of claim 6 1 further comprising determining if the first and second code assembly is a member assemblies are members of the at least one application.

**9. (Cancelled)**

**10. (Currently Amended)** The method of claim 6 1 wherein satisfying at least one trust condition is based at least in part on evidence provided with the at least one application.

**11. (Currently Amended)** The method of claim 6 1 wherein satisfying

at least one trust condition is based at least in part on evidence external to the at least one application.

**12. (Cancelled)**

**13. (Currently Amended)** The method of claim 6 1 wherein satisfying at least one trust condition is based on evidence from user interaction.

**14. (Currently Amended)** The method of claim 6 1 wherein satisfying at least one trust condition is based on evidence from evaluation of previous trust decisions.

**15. (Cancelled)**

**16. (Cancelled)**

**17. (Currently Amended)** A computer program product encoding a computer program for executing on a computer system a computer process, the computer process comprising:

receiving a manifest defining a plurality of first and second code assemblies that are members of at least one application, wherein the manifest

defines at least one trusted application and application evidence for making a trust decision;

evaluating the application evidence to determine if the at least one application is trusted; and

generating a first and a second permission grant set for each the first and the second code assembly, respectively, that is a member are members of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application;

passing the permission grant to a run-time call stack;

calling the second code assembly by the first code assembly, the second code assembly attempting access of a protected file; and

calculating an intersection of the first and the second permission grant sets to determine whether the access to the protected file is permitted.

**18. (Currently Amended)** The computer program product of claim 17 wherein the computer process further comprises the manifest further defining a plurality of code assemblies and evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

**19. (Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence based at least in part on an XrML license.

**20. (Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

**21. (Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

**22. (Cancelled)**

**23. (Cancelled)**

**24. (Currently Amended)** The computer program product of claim 22  
17 wherein the computer process further comprises determining if the first and  
~~second code assembly is a member assemblies are members~~ of the at least one

application.

**25. (Cancelled)**

**26. (Currently Amended)** The computer program product of claim 22  
17 wherein the computer process is based at least in part on evidence provided  
with the at least one application.

**27. (Currently Amended)** The computer program product of claim 22  
17 wherein the computer process is based at least in part on evidence external  
to the at least one application.

**28. (Cancelled)**

**29. (Currently Amended)** The computer program product of claim 22  
17 wherein the computer process is based on evidence from user interaction.

**30. (Currently Amended)** The computer program product of claim 22  
17 wherein the computer process is based on evidence from evaluation of  
previous trust decisions.

**31. (Cancelled)**

**32. (Cancelled)**

**33. (Currently Amended)** A system comprising:

a manifest defining first and second code assemblies that are members of at least one application;

application evidence to determine whether the at least one application is trusted; and

a loader to load the first and the second code assemblies into a run-time call stack, with the first code assembly calling the second code assembly, the second code assembly attempting access of a protected file; and

a policy manager to evaluate the application evidence relative to at least one condition, wherein the policy manager generates a first and second permission grant set for each the first and the second code assembly, respectively, that is-a member are members of the at least one application if the application evidence satisfies the at least one condition specified in a security policy specification for trusting the at least one application, wherein the security policy specification defines multiple policy levels, and wherein permissions are granted on a computer system based on the permission grant set, the policy manager further calculating an intersection of the first and the second

permission grant sets to determine whether the access to the protected file is permitted.

**34. (Original)** The system of claim 33 further comprising an XrML program authorization module operatively associated with the policy manager for evaluating application evidence including at least one XrML license.

**35. (Original)** The system of claim 33 wherein the policy manager evaluates evidence at a group level, an application level, and a code assembly level before the at least one application is executed.

**36. (Cancelled)**

**37. (Currently Amended)** The system of claim 33 wherein the policy manager further determines if the first and second code assembly is a member assemblies are members of the at least one application.

**38. (Original)** The system of claim 33 wherein the application evidence is provided with the at least one application.

**39. (Original)** The system of claim 33 wherein the application

evidence is provided external to the at least one application.

**40. (Original)** The system of claim 33 wherein the application evidence includes at least an XrML license.

**41. (Original)** The system of claim 33 wherein the application evidence includes evidence provided via user interaction.

**42. (Original)** The system of claim 33 wherein the application evidence includes evidence from the evaluation of previous trust decisions.

**43. (Original)** The system of claim 33 further comprising a security policy specification defining at least one trust condition for an application component, wherein the policy manager evaluates the at least one trust condition in the security policy specification.

**44-48. (Cancelled)**